CLAIMS

1) A procedure to avoid internet fraud that is carried out by means of a multi-key card in which Business X, a User and a Authorization Center intervene, characterized in that it includes the following steps:

requesting the legitimizing of Business X to operate with the Authorization Center;

checking out Business X in a database of the aforesaid Authorization Center, assigning Business X an identification code;

sending the list of future Business X users to the Authorization Center;

preparing the NICKS registry of Business X users and loading them into the proprietary database not available on the Web which step constitutes acceptance of the list of new users;

requesting a specific number of Multi-key cards for users qualified to operate by means of a note or purchase order;

generating in the A.C. a set consisting of a specific quantity of Multi-key cards, assigning a unique number to each set and another unique number to each card, relating this card code with the user's NICK;

distributing the aforementioned Multi-key cards to the corresponding users in a personalized manner, by means of a

form that possesses an organic security seal where the user must sign and leave his fingerprint;

updating information for the delivery of cards and returning this information to the A.C. by means of the security forms;

qualifying the NICKS of the users who have received the Multi-key card, thus up-dating the cards qualified; and

confirming the qualification to the recognized users.

2) The procedure to avoid Internet fraud, according to claim 1, characterized in that the following step consists of the authentication of user identity by means of a web page including the following steps:

entering the official legitimized web page, Business X requests entry to the portal of the Authorization Center by means of a link and, once entered therein, enters the NICK + a PIN of its Multi-key card;

Printing via the C.A. Web server the NICK + the PIN to a bar code, and sending it to the A.C. database, the database without an open connection where a laser reader connected to the database reads the data printed before and verifies whether the NICK are authorized, if the PIN entered belongs to that NICK and if the PIN entered has not been used before, authorizing the operation if the 3 verifications are positive or denying the operation if some of the aforesaid 3 verifications are negative;

the aforesaid server without open connection prints the result of the verification and sends it to the Web server, where another laser reader connected to the Web server reads the results of the verification, authorizing or denying the operation requested by the user.

3) The procedure to avoid Internet fraud according to claim 1, characterized in that the following step consists of the authentication of user identity by means of a Call Center including the following steps:

requesting legitimization as a Business X user by means of a telephone call to a Call Center,

in response to the Call Center operator the user reports his user NICK + a PIN code from his Multi-key card, data that will be entered by the operator into the system that makes the verification of such data available,

the system verifies that the NICK is qualified, that the PIN corresponds to the NICK and that the aforesaid PIN has not been used, authorizing the operation if the 3 verifications are positive or denying the authorization if any of the aforesaid 3 verifications are negative;

once the verification has been realized, giving a response to the request for legitimization of identity to the user who requests it by telephone and invalidates further use of the NICK + PIN combination for a future operation.

4) The procedure to avoid Internet fraud according to claim 2, characterized in that the PIN entered by the user has limited temporary validity.

5) The procedure to avoid Internet fraud according to claim 2, characterized in that the PIN entered by the user has a color determined as a function of the category of the user who holds the card.

6) The procedure to avoid Internet fraud according to claim 1, characterized in that the step of generating the Multi-key cards includes the additional steps of:

generating the cards in sets and assigning to each a unique alphanumeric card code of X characters (numbers, capital letters and/or lower-case letters), the system verifying that there is no identical code in the isolated database not available on the network;

generating a random alphanumeric code of variable length that will be utilized as a PIN;

repeating the operation as many times as the Multi-key card contains PINs so the system can verify that a PIN is not repeated in the same card;

assigning the user NICK to the code of the Multi-key card and keeping the information in the Authorization Center Database, thus authorizing this Multi-key card.

7) A multi-key card to avoid Internet fraud to be used in accordance with the method of claim 1, characterized as being of the usual size of magnetic cards, having imprinted thereon the user's NICK, a variable series of PINs (alphanumeric codes) hidden by a scratch-off type protective cover, a unique set code identifier issued by the Authorization Center printer at the time of generating a specific set of cards for Business X, and a card code identifier consisting of a unique alphanumeric code of X characters which identify that Multi-key card, relating it to the user and to the PINs he is authorized to use; as well as the fact that the front of the card may contain space for advertising.

8) The multi-key card according to claim 7, characterized by the fact that the NICK with regard to the Multi-key card comes printed and hidden by a scratch-off type protective cover.

9) The multi-key card according to claim 7, characterized by the fact that the NICK with regard to the Multi-key card comes printed on a removable plastic strip.

10) The multi-key card according to claim 7 characterized by the fact that the Multi-key card comes wrapped in shrink-seal cellophane.